DMP:AFM
F. #2017R00891

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF (1) ONE APPLE IPHONE MODEL 7 PLUS WITH FCC ID BCG-E3092A, (2) ONE SAMSUNG GALAXY CELLULAR PHONE WITH SERIAL NUMBER RF8HB0F3LQR; (3) ONE LG CELLULAR PHONE WITH SERIAL NUMBER 606CQZP0127869; (4) ONE APPLE IPHONE MODEL 5 WITH FCC ID BCG-E2599A AND IMEI 013335007373801; (5) ONE TRACFONE MODEL A466BG CELLULAR PHONE WITH IMEI 014866001605425; (6) ONE APPLE MACBOOK WITH SERIAL NUMBER C1MQ4R2YG940; AND (7) ONE APPLE MACBOOK WITHOUT INDIVIDUAL IDENTIFIERS, ALL CURRENTLY LOCATED IN THE CUSTODY OF THE DEPARTMENT OF HOMELAND SECURITY – HOMELAND SECURITY INVESTIGATIONS IN THE EASTERN DISTRICT OF NEW YORK	APPLICATION FOR A SEARCH WARRANT FOR ELECTRONIC DEVICES Case No. 17M458

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, James G. Masso, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of

property described in Attachment A—specifically, electronic devices—which are currently in law enforcement possession, and the extraction from the electronic devices of electronically stored information described in Attachment B.

2. I am a Special Agent with the Department of Homeland Security – Homeland Security Investigations ("HSI"). I have been a Special Agent for approximately two years. I have been involved in the investigation of numerous cases involving searches and forensic review of phones and other electronic devices.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

4. The property to be searched consists of the following electronic devices (hereinafter the "DEVICES"): (1) one Apple iPhone Model 7 Plus with FCC ID BCG-E3092A (the "Powell Arrest Phone"), (2) one Samsung Galaxy cellular phone with serial number RF8HB0F3LQR (the "Bedroom Galaxy"); (3) one LG cellular phone with serial number 606CQZP0127869 (the "LG"); (4) one Apple iPhone Model 5 with FCC ID BCG-E2599A and IMEI 013335007373801 (the "Bedroom iPhone"); (5) one TracFone Model A466BG cellular phone with IMEI 014866001605425 (the "TracFone"); (6) one Apple Macbook with serial Number C1MQ4R2YG940; and (7) one Apple Macbook without individual identifiers. The DEVICES are currently in the custody of the Department of Homeland Security – Homeland Security Investigations ("HSI") at John F. Kennedy International Airport in Queens, New York, within the Eastern District of New York.

5. The applied-for warrant would authorize the search and forensic examination of the DEVICES to seize the items further described in Attachment B.

PROBABLE CAUSE

I. Background

6. Agents of HSI have been investigating multiple elder fraud schemes perpetrated by Lorindo Powell ("Powell") and Tavoy Malcolm ("Malcolm"). Among other schemes, Powell and Malcolm conspired (1) to defraud a 77-year-old New Jersey resident ("Jane Doe 1") of the majority of her income for more than a decade by inducing her to pay purported "fees" connected to supposed investment-related windfalls, and (2) to defraud a 91-year-old New Jersey resident ("Jane Doe 2") of $23,000 in purported fees connected to supposed lottery winnings.

7. On May 9, 2017, the Honorable Cheryl L. Pollak, United States Magistrate Judge for the Eastern District of New York, authorized arrest warrants for Powell and Malcolm pursuant to a criminal complaint charging them with wire and bank fraud.

II. The Use of Cellular Phones and Computers in the Charged Frauds

8. The charged wire and bank frauds involved extensive use of cellular telephones. Powell and Malcolm used a prepaid cellular telephone to exchange more than 500 calls with Jane Does 1 and 2 during the first three months alone of 2017. Powell also had at least two postpaid cellular telephones, one that he appears to have reserved for personal use and one that he used to communicate with Jane Doe 1 during March and April 2017.

9. The charged wire and bank frauds also involved elaborate fraudulent sweepstakes notifications, which Powell and Malcolm sent to their victims. Based on my training and experience, these notifications appear to have been designed through the use of computers. In addition, agents have reviewed messages between Powell and Malcolm discussing the use of commercial printing services.

III. Malcolm's Arrest and the Search of Malcolm's Phone

10. Malcolm was arrested on May 11, 2017 in the Bronx, New York.

11. At the time of her arrest, Malcolm had a cellular phone on her person (the "Malcolm Phone"), which she gave officers consent to search.

12. Agents reviewed the Malcolm Phone and found numerous messages between Malcolm and Powell regarding the charged frauds.

13. They also found numerous messages discussing other uncharged frauds—messages in which Malcolm and Powell shared third parties' financial information, discussed receiving and sending money transfers, and shared Western Union receipts.

IV. Powell's Arrest and the Search of Powell and Malcolm's Apartment

14. Powell was arrested on May 12, 2017 after he deplaned from a flight at John F. Kennedy International Airport in Queens, New York. At the time of Powell's arrest, he was returning from a trip to Las Vegas during which he communicated with Jane Doe 1 by cellular phone. Powell had the Powell Arrest Phone on his person at the time of his arrest.

15. At the time of their respective arrests, Powell and Malcolm both resided in an apartment in Guttenberg, New Jersey (the "Apartment"). They shared the Apartment with a third person, Powell's sister, who is on pretrial supervision after having been charged in

this district on October 17, 2016 with cocaine importation and conspiracy to import cocaine.

16. Simultaneously with Malcolm's arrest, agents executed a search warrant at the Apartment. In the bedroom, they found (among other items) handwritten notes containing a known victim's personal information and a handwritten "script" to be used in calling victims and pretending to be a Citibank representative.

17. Agents also found a number of cellular phones at the Apartment. In the bedroom, they found the Bedroom Galaxy and the Bedroom iPhone. They found the LG on a hallway table and the TracFone on the living room floor.

18. In addition, agents found two laptop computers at the Apartment; an Apple Macbook laptop with serial number C1MQ4R2YG940, which they found on the kitchen table, and an older Apple Macbook without individual identifiers, which they found inside a bag in a closet.

19. Based on the foregoing evidence, there is probable cause to believe that information on the DEVICES will produce evidence probative of the crimes under investigation. Based on my training and experience, I am aware that individuals who commit financial fraud and identity theft often store evidence of their crimes on their mobile phones, including evidence of planning the frauds, communications about collecting and sending the proceeds, images of financial statements and money transfer records, and notes containing victims' financial information.

20. Based on my training and experience, I know that the DEVICES have been stored in a manner in which their contents are, to the extent material to this investigation, in

substantially the same state as they were when the DEVICES first came into the possession of HSI.

TECHNICAL TERMS

21. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

f. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

g. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

22. Based on my training, experience, and research, I know that the DEVICES have capabilities that allow them to serve as wireless telephones, digital cameras, portable media players, GPS navigation devices, and PDAs. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

23. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been

viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

24. There is probable cause to believe that things that were once stored on the DEVICES may still be stored there, for at least the following reasons:

h. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

i. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

j. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it.

To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

k. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

25. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the DEVICES were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the DEVICES because:

l. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

m. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

n. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

o. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

p. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

26. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the DEVICES consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the DEVICES to human inspection in order to determine whether it is evidence described by the warrant.

27. *Manner of execution.* Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

28. I submit that this affidavit supports probable cause for a search warrant authorizing the search of the devices described in Attachment A to seize the items described in Attachment B.

Respectfully submitted,

James G. Masso
Special Agent
Department of Homeland Security –
Homeland Security Investigations

S| Pohorelsky

THE HONORABLE VIKTOR V. POHORELSKY
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

ATTACHMENT A

The property to be searched consists of the following electronic devices (hereinafter the "DEVICES"): (1) one Apple iPhone Model 7 Plus with FCC ID BCG-E3092A; (2) one Samsung Galaxy cellular phone with serial number RF8HB0F3LQR; (3) one LG cellular phone with serial number 606CQZP0127869; (4) one Apple iPhone Model 5 with FCC ID BCG-E2599A and IMEI 013335007373801; (5) one TracFone Model A466BG cellular phone with IMEI 014866001605425 (the "TracFone"); (6) one Apple Macbook with serial Number C1MQ4R2YG940; and (7) one Apple Macbook without individual identifiers. The DEVICES are currently in the custody of the Department of Homeland Security – Homeland Security Investigations ("HSI") at John F. Kennedy International Airport in Queens, New York, within the Eastern District of New York.

This warrant authorizes the search and forensic examination of the DEVICES to seize the items further described in Attachment B.

ATTACHMENT B

1. All records on the DEVICES described in Attachment A that relate to violations of 18 U.S.C. §§ 1028, 1343 or 1344 (the "SUBJECT OFFENSES") and involve LORINDO POWELL or TAVOY MALCOLM for the period from January 1, 2000 to the present, including:

a. Any and all records, including phone logs, notes, correspondence, text messages, electronic mail, chat logs, and other communications or documents, related to the violation of the Subject Offenses;

b. Any and all communications and evidence of communications by, between, and among TAVOY MALCOLM, LORINDO POWELL, and other participants in the Subject Offenses and the Subject Schemes;

c. all bank records, checks, credit card bills, account information, and other financial records;

d. any documents used to notify victims of sweepstakes or lottery winnings, investment proceeds, or other windfalls; and

e. any documents related to telemarketing.

2. Evidence of user attribution showing who used or owned each of the DEVICES at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.